(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 October 2001 (04.10.2001)

PCT

(10) International Publication Number
WO 01/74053 A1

(51) International Patent Classification[7]: H04N 1/32

(21) International Application Number: PCT/GB01/01088

(22) International Filing Date: 14 March 2001 (14.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0007330.4 28 March 2000 (28.03.2000) GB

(71) Applicants *(for all designated States except US)*: **SOFTWARE 2000 LIMITED** [GB/GB]; The Magdalen Centre, Oxford Science Park, Oxford, Oxfordshire OX4 4GA (GB). **SIGNUM TECHNOLOGIES LIMITED** [GB/GB]; 6 Thorney Leys Business Park, Witney, Oxford, Oxfordshire OX8 7GE (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HARRIS, Anthony, William** [GB/GB]; 1 Stable Court, Shaw, Berkshire RG14 2DT (GB). **HILTON, David** [GB/GB]; 12 Harveys Lane, Winchombe, Gloucestershire GL54 5QT (GB).

(74) Agent: **LIND, Robert**; Marks & Clerk, 4220 Nash Court, Oxford Business Park South, Oxford, Oxfordshire OX4 2RU (GB).

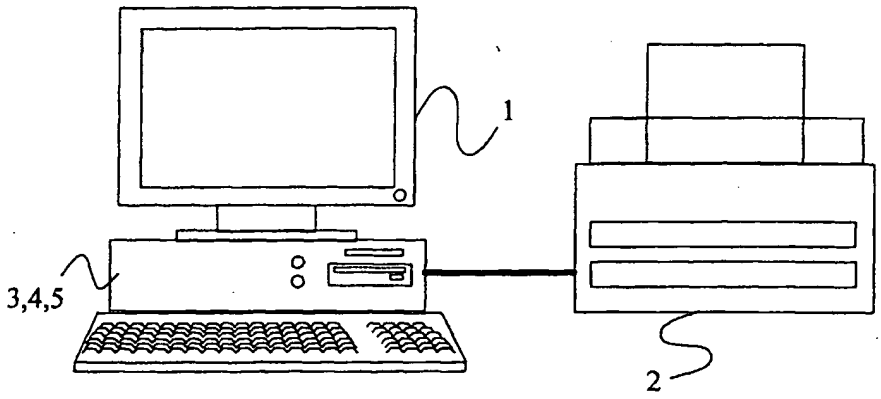
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DOCUMENT MARKING



(57) Abstract: A method of incorporating a fingerprint into a printed work, which fingerprint is substantially invisible to the naked eye but can be recognised by image processing techniques. The method comprises the steps of sending digital data corresponding to an image to be printed to a printer driver (5), incorporating at least one fingerprint into the data during processing by the printer driver (5), and sending the data processed by the printer driver (5) to a printer (2).

WO 01/74053 A1

DOCUMENT MARKING

The present invention relates to document marking and in particular to a method, apparatus, and computer program for incorporating a unique identifier into a printed document.

The counterfeiting of bank notes and of other intrinsically valuable documents has always been a serious problem which has exercised the minds of individuals, companies, and governments alike. The counterfeiting of bank notes in the US alone is estimated to run at 70 million dollars per annum. Recently, the problem of counterfeiting has increased due to the availability of high quality, low cost digital printers and scanners, and the quality of counterfeits produced by such means is approaching that which can be achieved by conventional offset lithography equipment. It will be appreciated that the potential for damage is enormous, if every home and office is capable of producing extremely high quality forgeries.

There is only a limited amount which can be done to stop a person producing counterfeits if they have the desire to do so. Attempts have been made to produce bank notes which are in some ways resistant to photocopying or digital scanning, but these have met with only limited success and at best achieve only some degree of degradation in the copies or scanned image. In the light of this, enforcement agencies still rely on more conventional methods of policing. However, in the event that a suspected counterfeiter is apprehended by the authorities, there is often a problem in obtaining sufficient information to achieve a successful prosecution. Particularly where counterfeits are prepared using a home PC and printer, it is very easy for the counterfeiter to erase any trace of his activities.

One solution to the problem of obtaining evidence for use in a court of law, involves incorporating a "fingerprint" into printed or copied documents which is unique to the equipment used to prepare the document. For example, certain photocopiers comprise a chip on which is encoded a unique identifier which is incorporated into a copied document in such a way that, whilst substantially invisible to the naked eye, it can be

discerned using special imaging technology. The requirement for a special chip adds to manufacturing costs however and, whilst contributing only a relatively small fraction of the total cost of a photocopier, would be more significant if the same technology were to be incorporated into desktop printers.

It is an object of the present invention to overcome or at least mitigate the disadvantages of existing anti-counterfeiting measures noted above. In particular, it is an object of the present invention to provide a relatively simple and low cost anti-counterfeiting means which may be incorporated into desktop PCs, workstations, and the like. It is also an object of the present invention to provide a mechanism for combating the pirating of printer driver software and software components.

According to a first aspect of the present invention there is provided a method of incorporating a fingerprint into a printed work, which fingerprint is substantially invisible to the naked eye but can be recognised by image processing techniques, the method comprising the steps of:

sending digital data corresponding to an image to be printed to a printer driver;

incorporating at least one fingerprint into the data during processing by the printer driver by altering the colour and/or intensity of pixels of the image data; and

sending the data processed by the printer driver to a printer.

The printer driver represents a "point" through which all data to be printed must pass, and is aware of both the format of the data received from the printing application and of the format of data required by the printer. It therefore represents a more comprehensive solution than could be achieved by incorporating a fingerprint into image data at say an image scanner (using either a software or a hardware solution) or by way of a specific application (e.g. Microsoft Word™). Implementing a solution at the operating system level is also unlikely to be feasible as many operating systems are already in use and it would be difficult or impossible to "retrofit" a fingerprint solution. In contrast, printer drivers tend to be replaced or updated (e.g. to introduce bug fixes) fairly often, and so a solution introduced at this level would percolate through computer systems fairly rapidly.

Preferably, the step of incorporating at least one fingerprint into the image data is carried out automatically by the printer driver substantially without any possibility for intervention by the user of the equipment on which the printer driver resides.

Preferably, said fingerprint corresponds to an identification (e.g. serial number) associated with the host computer system (e.g. the ID of the host computer BIOS, the operating system ID or a chip ID), the printer, or the printer driver. More preferably, the identification is a unique identifier. The method of the present invention may comprise the steps of determining whether or not the printer has an ID which can be used as said fingerprint and, if not, determining whether or not the computer system has a usable ID. The latter step may comprise determining whether or not the computer operating system has an ID which can be used as said fingerprint and, if not, determining whether or not the motherboard or microprocessor of the computer system has a usable ID. The step(s) of determining a suitable fingerprint may be carried for example out during the installation of the printer driver, or each time the printer driver receives a new print job.

The fingerprint may be incorporated into the image data to be printed, in an encrypted form so that it can only be determined after image processing and decryption steps. The use of encryption may prevent unauthorised parties from determining the source of a printed document. Encryption may be achieved, for example, using an encryption key based algorithm.

In certain embodiments of the present invention, the fingerprint may be subjected to a one way hashing operation using a hashing function prior to incorporation into the image data. This would make it difficult or impossible to reverse the process, i.e. to determine the fingerprint from data recovered from a printed work. However, it would be possible to associate a printed work to a computer system if the computer system is available. The use of a fingerprint which is generated using multiple IDs, e.g. an ID of the printer and an ID of the printer driver, may result in an increased level of security.

Preferably, the step of incorporating a fingerprint into the image data step is carried out after the received image data has been rasterised by the printer driver. More preferably,

the luminance of pixels is varied, whilst the chrominance remains substantially unchanged. This may be achieved, in a colour image, by varying each of the Red, Green, and Blue components.

Preferably, the pixels are altered prior to rendering the image data.

Preferably, the level by which the image data is altered to incorporate the fingerprint depends upon the quality of the image to be printed. The level of alteration may vary with one or more of the following; the printing resolution, paper quality, and bit depth of the image.

The level of alteration may vary across the image to be printed. A single fingerprint may be repeated at intervals across the image to be printed, or different fingerprints may be incorporated into a single image.

According to a second aspect of the present invention there is provided a computer memory encoded with executable instructions representing a printer driver computer program for causing a computer system to output digital data to a printer, wherein the resulting printed image comprises an image corresponding to the image data received by the printer driver and a fingerprint which is substantially invisible to the naked eye but can be recognised by image processing techniques.

Preferably, said computer program is arranged to be inoperable in the event that software code relating to said fingerprint or to the incorporation of said fingerprint into an image to be printed is tampered with.

According to a third aspect of the present invention there is provided a method of combating the counterfeiting of printed works, the method comprising incorporating into printer driver software, software code for causing a fingerprint to be incorporated into image data processed by that printer driver, which fingerprint results in a change in the image when printed which is substantially invisible to the naked eye but can be detected by image processing techniques.

According to a fourth aspect of the present invention there is provided a method of combating the pirating of driver software or images, the method comprising incorporating into printer driver software, software code for causing a fingerprint to be incorporated into image data processed by that printer driver, which fingerprint results in a change in the image when printed which is substantially invisible to the naked eye but can be detected by image processing techniques.

According to a fifth aspect of the present invention there is provided a computer system having memory means storing a computer program according to the above second aspect of the present invention, and processing means for executing said program so as to cause a fingerprint to be incorporated into an image printed from the computer system.

According to a sixth aspect of the present invention there is provided a method of incorporating a fingerprint into printed image, which fingerprint is substantially invisible to the naked eye, the method comprising encrypting the fingerprint using a one-way hashing function prior to its incorporation into image data to be printed, and subsequently printing the modified image data, wherein the fingerprint may only be recovered from the printed image using a knowledge of the hashing function.

For a better understanding of the present invention and in order to show how the same may be carried into effect reference will now be made, by way of example, to the accompanying drawings, in which:

Figure 1 illustrates a typical computer system; and

Figure 2 illustrates in block diagram form a printing portion of the computer system of Figure 1.

There is illustrated in Figure 1 a personal computer (PC) 1 and a digital printer 2. The PC is controlled by a software operating system 3 such as Microsoft Windows 98™, LINUX, or UNIX™, and is arranged to run applications 4 such as Microsoft Word™, Adobe PhotoShop™ and the like. In use, data to be printed is transferred from an application 4, under the control of the operating system 3, to a software module known as a printer driver 5. Printer drivers are often printer specific and are typically installed

into a PC from a printer manufacturer's CD ROM or from a driver library provided with the operating system. Printer drivers may be updated, e.g. to add new features or to fix bugs, using executable files supplied by the driver manufacturers.

The printer driver 5 typically takes image data to be printed (the image may correspond to text, pictures, diagrams, etc), and converts this into a grid (or raster space) of pixel values, where each value represents the colour of the image at that point in the grid. This process is referred to as "rasterising". Following the rasterising of the image data, the data is modified in order to incorporate into the image a unique fingerprint. This fingerprint is preferably a unique ID which is encoded into the printer hardware or software and which is detected by the printer driver 5 during its installation. The determined ID is stored in an appropriate secure location for later use by the printer driver 5. If the printer 2 has no useable ID, or the ID cannot be determined for any reason, the printer driver 5 may then try to identify a motherboard serial number or CPU serial number (as for example on the Intel Pentium III). If a usable ID still cannot be obtained, then the printer driver 5 may look for a hard disk serial number, an Ethernet MAC address (when the computer has a card with a non-null address), a hash value generated based on the bad sector map on the boot drive, a Plug and Play serial number (on PCs with PCI only), or an MS-DOS serial number (on PCs). If there is no convenient permanent value, then one may be generated, for example using CoCreateGuid (under MS Windows on a PC), and stored in the PC's registry or its equivalent, or in a custom generated file. A unique ID may also be generated using some combination of the listed codes. An advantage of using such a combination would be that even though a user changes some parts of his system, it may still be possible to link the fingerprint to remaining parts of the system.

Figure 2 illustrates schematically a printing system of the computer system of Figure 1. In essence, the printing system consists of a printer driver 5 which uses a set of data processing modules to process image data received from the operating system. A first of the modules used by the driver 5 is a rasterising module 6, the function of which has already been described above. The second module which receives the rasterised data from the rasterising module is a fingerprint application module 7.

The operation of the fingerprint module 7 will not be describer in detail here. Instead, reference should be made to International application no. PCT/GB/00491 in the name of Highwater FBI Ltd. Briefly, this document describes a method of incorporating a fingerprint into a printed image in such a way that the fingerprint is not readily visible to the naked eye, but can be determined by scanning and processing the printed image. The method uses a technique known as the "permutation" method and involves applying a code to modify the luminance (with the chrominance remaining substantially unchanged) of a sequence of pixels of the rasterised image data. Permutations of the code are applied in sequence to modify the entire image (alternatively, the process may be repeated for multiple tiled regions of the image). Orientation markers are incorporated into the image to allow analysis software to correctly orient the image. PCT/GB/00491 describes how the fingerprint may be recovered using a statistical analysis of a subsequently scanned version of the image, and the encryption key. The fingerprint module of the printer driver 5 uses the permutation technique, where the code used to modify the image data is generated using the fingerprint described above and an encryption key. Both the fingerprint and the encryption key are stored in secure block of memory and are retrieved by the fingerprint module when required.

The "strength" of the fingerprint may be scaled prior to its incorporation into the image in order to prevent the encrypted fingerprint from visibly altering the image quality (obviously any distortion of a printed image is undesirable). The strength may be determined on the basis of a number of factors including the resolution at which the printing occurs, the quality of the paper on which the image is to be printed, and the bit depth of the image data. The strength may vary across an image depending upon local conditions, e.g. the fingerprint is applied more heavily in noisy regions.

It will be appreciated that in order to be useful, the fingerprint module should be secure against tampering, e.g. to modify the fingerprint. A satisfactory level of security may be achieved, for example, by using the multiple storage and cross-referencing of the fingerprint, and/or storage of the fingerprint within a self-modifying driver.

The image data output from the fingerprint module 7 is passed by the printer driver 5 to a rendering module 8. A main function of the rendering module 8 is to convert the pixel

intensity data into corresponding halftone values (most printers are incapable of varying the intensity of a printed pixel, and so intensity variations are achieved by mixing colour and white pixels to an appropriate degree, a process known as "halftoning"). The halftone data is then passed to a formatting module 9 which arranges the data, and introduces formatting commands, into a form acceptable to the printer 2.

It is envisaged that the present invention may be adopted by organisations, such as the major world banks, as a means of combating the forgery of bank notes, bonds, certificates, and the like. The matching of an fingerprint found on a counterfeit document to a particular piece of software or hardware is likely to prove convincing evidence in a court of law.

It is also envisaged that manufacturers of printer drivers (or other software components) may use the present invention to combat the pirating of their software. Printer drivers and technologies such as halftoning and colour matching are critical to the success of print devices and require multiple man years to develop. Third parties are often tempted copy all or parts of drivers and to illegally attempt to pass them off as having developed them themselves. This problem may be combated by introducing of a hidden fingerprint into printed output as described above.

It will be appreciated by the person of skill in the art that various modifications may be made to the above described embodiment without departing from the scope of the present invention. For example, in order to overcome fears that an innocently printed document may be traced back to an originating computer system or printer, a one-way hashing function may be used to encrypt a fingerprint in a printer driver. The operation of one-way hashing is described in "Applied Cryptography", Bruce Schneier, 2ed, 1996, John Wiley & Sons, p30-31 and 351-354, and results in a value from which the fingerprint cannot be derived without the knowledge of the hashing function. Thus, assuming that the hashing function is only contained in the printer driver, authorities would only be able to match a printed document to a computer system or printer if they have access to the printer driver. The fingerprint may be combined with a unique identity known only to the printer driver, prior to hashing, in order to significantly

reduce the possibility of someone deriving the fingerprint by applying all possible fingerprints to recovered image data.

CLAIMS:

1. A method of incorporating a fingerprint into a printed work, which fingerprint is substantially invisible to the naked eye but can be recognised by image processing techniques, the method comprising the steps of:

sending digital data corresponding to an image to be printed to a printer driver;

incorporating at least one fingerprint into the data during processing by the printer driver by altering the colour and/or intensity of pixels of the image data; and

sending the data processed by the printer driver to a printer.

2. A method according to claim 1, wherein the step of incorporating at least one fingerprint into the image data is carried out automatically by the printer driver substantially without any possibility for intervention by the user of the equipment on which the printer driver resides.

3. A method according to claim 1 or 2, wherein said fingerprint corresponds to an identification associated with the host computer system or the printer.

4. A method according to claim 3, wherein the identification is selected from one of the following: a printer hardware or software ID, computer motherboard serial number, a CPU serial number, a hard disk serial number, an Ethernet MAC address, a hash value generated based on the bad sector map on the boot drive, a Plug and Play serial number, or an MS-DOS serial number, or an identification generated by the printer driver.

5. A method according to claim 4, wherein the identification is generated using two or more of the listed numbers.

6. A method according to any one of the preceding claims, wherein a fingerprint is identified during installation of the printer driver.

7. A method according to any one of the preceding claims, wherein the fingerprint is incorporated into the image to be printed in an encrypted form so that it can only be determined after image processing and decryption steps.

8. A method according to claim 7 and comprising subjecting the fingerprint to a one way hashing operation using a hashing function, prior to incorporation into the image data.

9. A method according to any one of the preceding claims, wherein the luminance of pixels is varied, whilst the chrominance remains substantially unchanged.

10. A method according to any one of the preceding claims, wherein the pixels are altered after the image data has been rasterised by the print driver.

11. A method according to any one of the preceding claims, wherein the pixels are altered prior to rendering the image data.

12. A method according to any one of the preceding claims, wherein the level by which the image data is altered to incorporate the fingerprint depends upon the quality of the image to be printed.

13. A computer memory encoded with executable instructions representing a printer driver computer program for causing a computer system to output digital data to a printer, wherein the resulting printed image comprises an image corresponding to the image data received by the printer driver and a fingerprint which is substantially invisible to the naked eye but can be recognised by image processing techniques, said program causing introducing the fingerprint into the image data by altering the colour and/or intensity of pixels of the image data.

14. A method according to claim 13, wherein said computer program is arranged to be inoperable in the event that software code relating to said fingerprint or to the incorporation of said fingerprint into an image to be printed is tampered with.

15. A method of combating the counterfeiting of printed works, the method comprising incorporating into printer driver software, software code for causing a fingerprint to be incorporated into image data processed by that printer driver, which fingerprint results in a change in the image when printed which is substantially invisible to the naked eye but can be detected by image processing techniques.

16. A method of combating the pirating of driver software or images, the method comprising incorporating into printer driver software, software code for causing a fingerprint to be incorporated into image data processed by that printer driver, which fingerprint results in a change in the image when printed which is substantially invisible to the naked eye but can be detected by image processing techniques.

17. A computer system having memory means storing a computer program according to the above second aspect of the present invention, and processing means for executing said program so as to cause a fingerprint to be incorporated into an image printed from the computer system.

18. A method of incorporating a fingerprint into printed image, which fingerprint is substantially invisible to the naked eye, the method comprising encrypting the fingerprint using a one-way hashing function prior to its incorporation into image data to be printed, and subsequently printing the modified image data, wherein the fingerprint may only be recovered from the printed image using a knowledge of the hashing function.

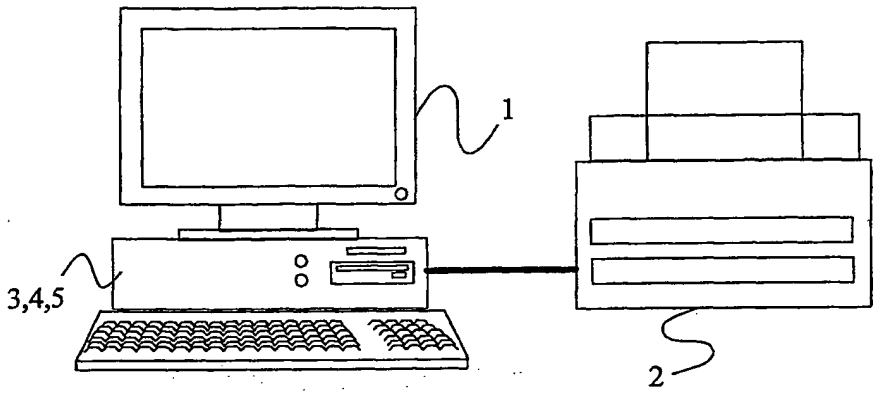


Figure 1

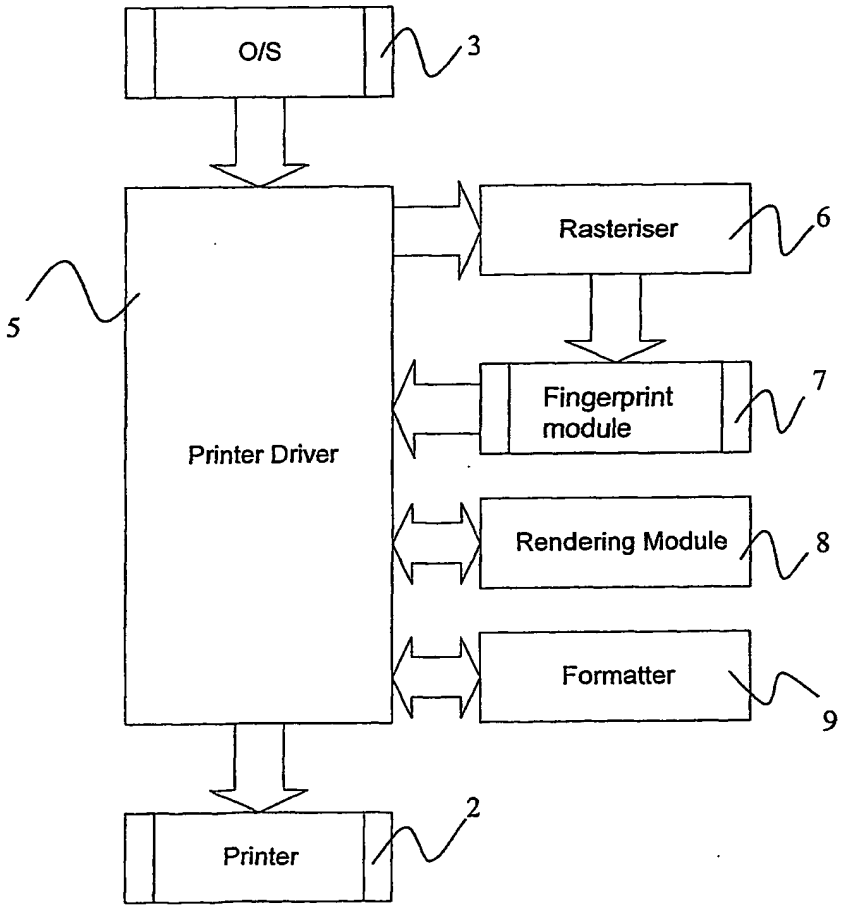


Figure 2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/[illegible] 1/01088

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N1/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N G06F G06T

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 644 682 A (WEINBERGER JOSEPH ET AL) 1 July 1997 (1997-07-01) abstract column 1, line 61 -column 2, line 25 column 3, line 30 - line 38 column 4, line 48 -column 5, line 4 column 9, line 10 - line 23 figure 3 claim 1	1,2,7-9, 13,15,16
Y	WO 96 27259 A (HIGHWATER FBI LIMITED ;HILTON DAVID (GB)) 6 September 1996 (1996-09-06) page 2, line 25 - line 35 page 4, line 28 - line 34 page 7, line 31 - line 37	1,2,7-9, 13,15,16

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 June 2001	04/07/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Stoffers, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/ 1/01088

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 97 02522 A (HIGHWATER FBI LIMITED ;HILTON DAVID (GB)) 23 January 1997 (1997-01-23) abstract	1-19
A	WOLFGANG R B ET AL: "Overview of image security techniques with applications in multimedia systems" PROCEEDINGS OF THE SPIE, 4 November 1997 (1997-11-04), XP002104655 * the whole document *	1-18
A	MINTZER F ET AL: "EFFECTIVE AND INEFFECTIVE DIGITAL WATERMARKS" PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON IMAGE PROCESSING.,US,LOS ALAMITOS, CA: IEEE COMPUTER SOCIETY, 1997, pages 9-12, XP000780838 ISBN: 0-8186-8184-5 * the whole document *	1-18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US01/01088

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5644682 A	01-07-1997	NONE	
WO 9627259 A	06-09-1996	AU 4885296 A	18-09-1996
		DE 69612658 D	07-06-2001
		EP 0813788 A	29-12-1997
		JP 11501173 T	26-01-1999
WO 9702522 A	23-01-1997	AU 6233996 A	05-02-1997
		DE 69607844 D	25-05-2000
		DE 69607844 T	22-02-2001
		EP 0838050 A	29-04-1998